Exhibit 6

KAISERDILLON PLLC

1099 14TH ST. NW
8TH FLOOR WEST
WASHINGTON, DC 20005
(202) 640-2850
WWW.KAISERDILLON.COM

June 8, 2020

VIA ELECTRONIC MAIL

Mr. Jay Prabhu
Mr. William G. Clayman
Assistant United States Attorneys
United States Attorney's Office for the Eastern District of Virginia
2100 Jamieson Avenue
Alexandria, VA 22314
Jay.Prabhu@usdoj.gov
William.G.Clayman@usdoj.gov

Re: *United States v. Zackary Ellis Sanders*, 1:20-mj-00114

Dear Jay and Bill,

As you know, our law firm represents Zackary Sanders in case 1:20-mj-00114. This letter is to follow up on our previous conversations with Bill regarding the search warrant in this case.[1] As noted at the conclusion of this letter, we are also requesting a meeting (or a call, at minimum) to discuss further the issues addressed below.

We believe the search warrant the government obtained in this case violated Mr. Sanders's rights under the Fourth Amendment. Special Agent Ford's affidavit contains numerous false statements that were directly relevant to the Court's probable cause determination. While we believe that the affidavit was facially deficient even if those statements had been true—which they were not—when the affidavit is corrected to reflect the true facts, the matter is not close. The good-faith exception to the warrant requirement accordingly does not apply. *See United States v. Gary*, 528 F.3d 324, 329 (4th Cir. 2008) (noting that the good faith exception does not apply where, *inter alia*, probable cause is based on false statements in the affidavit that were knowingly or recklessly made or where the affidavit does not provide a substantial basis for probable cause).[2]

[1] In an email on May 27, 2020, Bill cancelled a planned telephone call and informed us that the government is refusing to provide any further discovery in this matter pre-indictment.

[2] We have retained as an expert Dr. Matthew Miller, Assistant Professor Computer Science and Information Technology at the University of Nebraska at Kearney. Based on our discussions with Dr.

I. The reviewing court will find that the warrant lacked probable cause.

The central allegation supporting probable cause is contained in paragraph 23 of Special Agent Ford's affidavit. In that paragraph, Special Agent Ford alleges that an unnamed Foreign Law Enforcement Agency ("FLA") reported to the FBI that an Internet user with IP address [redacted] "accessed online child sexual abuse and exploitation material" on the target website on May 23, 2019. The remainder of the affidavit does not reflect that the FBI verified or corroborated the FLA's tip; to the contrary, Special Agent Ford appears to have accepted the information regarding the Internet user's alleged activities—and passed that information on to the Court via his affidavit—without any further investigation into the Internet user's conduct.[3]

Agent Ford's acceptance of the FLA tip at face value is not consistent with the dictates of the Fourth Amendment. Without further indication that the FBI corroborated the tip—which, based on our phone conversation with you, was itself minimal and bare-boned—the affidavit lacked facts needed to provide "a substantial basis for crediting the hearsay." *Jones v. United States*, 362 U.S. 257, 269 (1960), *overruled on other grounds by United States v. Salvucci*, 448 U.S. 83, 100 (1980). Nor was the hearsay from the tip "reasonably corroborated by other matters" that were within the affiant's knowledge. *Id.* The fact that this unnamed FLA allegedly had a history of providing reliable, accurate information in the past is not enough, without further corroboration, to support probable cause.[4]

There are at least three circumstances here that undermined the FLA's allegation that the Internet user accessed child pornography via the target website. They are: (1) the website was not exclusively dedicated to child pornography; (2) there was no allegation that the Internet user ever actually registered an account to the website; and (3) there was no specific description of the content the Internet user allegedly accessed.

First, the website is alleged to have contained (and did contain) legal and illegal content. The affidavit described the website as "a message board webpage" that included "sections and forums for posting to the website," as well as "a private message feature." (Affidavit ¶¶ 16, 18). In June 2016, a website administrator posted a topic entitled "Board Rules" in the "'Important Information' forum" that described the "Hurtcore" content of the site as including, among other things, "fighting, wrestling, bondage, spanking, pain, . . . gore." (Affidavit ¶ 19). These are descriptions of legal content. In July 2016, a message in the "Announcements' hyperlink" of the

---

Miller and the background of the case as we understand it, Dr. Miller is prepared to testify that critical assertions from Special Agent Ford's affidavit are false.

[3] As addressed below, it strongly appears that the statements regarding the FLA tip in paragraph 23 of the affidavit were false. In this section of our letter, however, we assume that paragraph 23 accurately characterized the tip.

[4] Although it is alleged that no U.S. law enforcement personnel participated in the investigative work that identified the IP address, the affidavit did not allege that the FBI ever subsequently sought to determine whether the Internet user had visited the website on any other occasions or that the FBI ever conducted any other independent investigative work to corroborate the tip from the FLA. If there were any such efforts that did not yield additional information supporting probable cause, that is exculpatory information that the government is obligated to disclose in time for Mr. Sanders to use for his defense, including his investigation of facts relevant to a motion to suppress and a motion for a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978).

target website stated that the website was "created to host videos, photos and discussions of 18 (twinks)[5] and younger of Hurtcore materials." (Affidavit ¶ 17).

Second, there was no allegation that the Internet user ever actually registered an account to the website. As the affidavit alleged, users were required to register to "see all forums" and "access the majority of the material." (Affidavit ¶ 25). Unlike the affidavit in the Playpen case in *United States v. Matish*, 193 F. Supp. 3d 585, 603 (E.D. Va. 2016), the affidavit in this case did not allege that any child pornography was visible on the website's homepage or accessible prior to registering an account and logging in; that the entirety, or even the majority, of the website was dedicated to child pornography; that the website homepage prohibited re-posting material from other websites; that the homepage referenced compressing large files for distribution; or that the website had a name suggestive of child pornography. These facts, rather than corroborating the FLA's tip, suggest there was a fair probability that the Internet user simply visited the website's homepage on May 23, 2019, without accessing any of the mix of legal or illegal content that could be available if a person were logged in.

And third, there was no specific description of the content the Internet user allegedly accessed. Other than paragraph 23, the affidavit does not provide any further description of the content the Internet user is alleged to have accessed. It appears Special Agent Ford simply accepted the FLA's conclusion that the content was in fact "child abuse and sexual exploitation material," and assumed that the content met the definition of child pornography under U.S. law, without conducting any further inquiry as to what that content consisted of. *Cf. United States v. Bosyk*, 933 F.3d 319, 322 (4th Cir. 2019), *cert. denied*, 140 S. Ct. 1124 (2020) (in the affidavit in support of a search warrant, the FBI described a message with numerous thumbnail images depicting a man sexually molesting a female toddler, which was unmistakably child pornography).

Without the tip from the FLA, there was no connection between the Internet user and the target website and no allegation that the Internet user actually accessed any illegal content. There were no facts from which to determine how the FLA identified the IP address information of the Internet user or how the FLA determined what content was accessed through that IP address.

This Court has held that "a magistrate may rely on law enforcement officers, who may draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them . . . *as long as the affidavit contains facts to support the law enforcement officer's conclusions*." *United States v. Matish*, 193 F. Supp. 3d 585, 602 (E.D. Va. 2016) (*citing United States v. Johnson*, 599 F.3d 339, 343 (4th Cir.2010)) (internal citations and quotations omitted) (emphasis added). However, generalized allegations about computers; the Internet; and how the Tor network functions, as well as postings on the website that the Internet user was not alleged to have accessed; the behavior of users on a different website that the Internet user was not alleged to have visited; and characteristics of individuals with a sexual interest in children or visual depictions of children (as described in

[5] The reasonable inference is that "18 (twinks)" referred to adults at least 18 years of age and that the website therefore included content of adults at least 18 years of age as well as discussion boards between people at least 18 years of age.

paragraphs 38-44 of the affidavit) that the Internet user was not alleged to have displayed or possessed do not establish any nexus between the Internet user and child pornography.

The Fourth Amendment requires that "[s]ufficient information . . . be presented to the magistrate to allow that official to determine probable cause; his action cannot be a mere ratification of the bare conclusions of others." *Illinois v. Gates*, 462 U.S. at 239. The affiant's recital of suspicion relayed from the foreign law enforcement agency to the FBI in Paragraph 23 of the affidavit was analogous to the "mere affirmation of suspicion and belief without any statement of adequate supporting facts" that has been rejected by the Supreme Court. *Nathanson v. United States*, 290 U.S. 41, 46 (1933) (affiant's statement that he had "cause to suspect and does believe" that smuggled liquor was present in a private home was insufficient to provide probable cause).

Given the lack of corroboration for the hearsay contained in paragraph 23, there was not "a substantial basis for determining . . . a search would uncover evidence of wrongdoing." *Illinois v. Gates*, 462 U.S. 213, 236 (1983). Assuming *arguendo* that paragraph 23 accurately described the tip (which it did not, *see infra*), the fact that the Internet user allegedly accessed child pornography on one occasion is not enough to reasonably infer that the person *intended or attempted* to view child pornography. (Affidavit ¶ 23). Nor is paragraph 23 enough to link the person, as the affiant claimed, to "an online community of individuals who regularly send and receive child pornography." (Affidavit ¶ 6). Where the Internet user is only alleged to have accessed illegal content on a single date without facts to show that the user registered an account, viewed or downloaded any content that the FBI was able to specifically describe, posted any content, or ever returned to the website, the most reasonable inference is that the Internet user *did not* intend or attempt to access child pornography. These facts are insufficient to support a search of someone's home, the contents of electronic storage devices within it, or any person located at the home.

Assuming *arguendo* that the Internet user knew what type of content the website might contain, the most reasonable inference is that the Internet user intended only to access legal content or engage in legal speech protected by the First Amendment. For example, had the user searched for "adult BDSM" or "adult hurtcore" using a Tor-based search engine, this website could have come up within the results. However, because search engines do not have login credentials, they cannot access or determine the substance of content that is only accessible via registration and login.

There were no facts from which to allege that the FBI ever investigated how the 16-or-56 character web address was conveyed to or encountered by the Internet user. The most reasonable inference is that the Internet user could have encountered the web address through a Tor-based search engine, discussion forums for consenting adults, directory sites featuring pornography of consenting adults, or other directory sites featuring legal content. Another reasonable inference is that the Internet user inadvertently accessed the website by mistyping even 1 character of the 16-or-56 character web address for another website that the user actually intended to visit, mistyping an address that another person told them, or clicking on a hyperlink whose label did not make clear what site or content it linked to. Most people have probably clicked on a link that turned out to be something different than what they anticipated and clicking on a link does not prove that someone was familiar with its contents (and this is particularly true with a Tor-browser where addresses are 16-or-56 characters).

Based on the four corners of the affidavit and the lack of sufficient facts to corroborate the hearsay from the FLA as detailed in Paragraph 23, the warrant lacked probable cause.

II. The good faith exception to the warrant requirement does not apply.

A. The FBI Special Agent misled the magistrate judge with false statements and material omissions.

1. Special Agent Ford falsely described the central basis for the warrant: the FLA tip.

It strongly appears that Special Agent Ford misled the magistrate judge on the single most important issue underlying the probable cause determination in this case: that the FLA tip alleged that the Internet user had in fact "accessed online child sexual abuse and exploitation material via [Hurtmeh]." Affidavit ¶ 23. That statement was false. As you are aware, the report Special Agent Ford completed to open the investigation into the IP address reflects that the FLA tip stated that the Internet user merely *accessed the website*. It did not allege that the Internet user accessed any content from the website (not to mention illegal content). In the FD-1057 from January 17, 2020, Special Agent Ford stated that the tip from the FLA was simply that the user "accessed [redacted]," the target website. In the affidavit from February 10, 2020, however, Agent Special Ford swore that the FLA tip stated that the Internet user had "accessed online child abuse and exploitation material via a website." (Affidavit ¶ 23).

FD-1057 Form	Affidavit in Support of Search Warrant
"In August 2019, the FBI received information from a foreign law enforcement agency . . . that the FLA identified a user who **accessed [redacted] [the name of website]** using IP address [redacted] at 02:06:48 UTC." (FD-1057 Form at 2) (emphasis added).	"In August 2019, a foreign law enforcement agency . . . notified the FBI that the FLA determined that on May 23, 2019, a user of IP address 98.169.118.39 **accessed online child sexual abuse and exploitation material via a website** (Affidavit ¶ 23) (emphasis added).

Special Agent Ford's false description of the FLA tip was plainly material to the issuance of the warrant. That the Internet user "accessed online child sexual abuse and exploitation material" is the single most important fact justifying the issuance of the warrant. Indeed, *this is the only incriminating fact contained in the affidavit*. When the misleading statement in paragraph 23 is corrected to reflect that the FLA tip merely stated that the Internet user visited the website (and only on a single occasion), it is abundantly clear that the warrant was not supported by probable cause. Given the centrality of Special Agent Ford's false statement in paragraph 23 to the Magistrate's probable cause determination, this false statement alone requires suppression of the warrant's evidentiary fruits.

2. Special Agent Ford knew or should have known that his statement that the FLA did not interfere with, access, search, or seize data from a computer in the United States was false.

Special Agent Ford also likely misled the Court regarding the activity of the FLA when he averred that "the foreign law enforcement agency had not interfered with, accessed, searched,

or seized any data from any computer in the United States in order to obtain that IP address information." (Affidavit ¶ 25). Based on our understanding—and as Dr. Miller will likely opine—the FLA would not have been able to identify the IP address *without* using the website to remotely interfere with, access, search, or seize data from the device with IP address [redacted] located in the United States.[6]

When people use Tor, they are anonymized such that law enforcement cannot readily identify them by their IP address because that IP address is not transmitted or shared in any retrievable way. Law enforcement must use an exploit in the software that the user is running on his or her computer to seize the IP address and other identifying information from that target computer directly, and a computer system that has been exploited could have been fundamentally altered in some way, which may cause the computer to crash, lose or alter data, not respond to normal input or it may alter any of the settings on that system. That is what must have happened here.

Such an invasion of a computer on these facts—for the reasons discussed in section 1 and including when there is no allegation that the Internet user provided any personally identifying information such as an email address, contact information, or credit card information—would have required a valid warrant. *Cf. United States v. Richardson*, 607 F.3d 357 (4th Cir.2010) (finding probable cause where investigation linked defendant's email accounts, which he used to distribute child pornography, to the address where the warrant was executed); *United States v. Goodwin*, 854 F.2d 33 (4th Cir.1988) (finding probable cause for anticipatory search warrant when defendant ordered child pornography and investigation verified that materials would be delivered to the address where warrant was executed). In any event, the fact that the affidavit falsely portrayed the FLA's activities requires suppression.

3. Special Agent Ford omitted material facts.

In addition to the two statements that were at a minimum misleading, Special Agent Ford omitted from the warrant material information, including information that he notably did record in the FD-1057. First, not only did the Internet user visit the website on a single date, there was a timestamp—for a single second, 02:06:48 UTC—that reflected when the Internet user allegedly accessed the website. As Dr. Miller would opine, the time stamp could reflect the extent of the activity the Internet user engaged in. Had Special Agent Ford included this timestamp, which he included in the FD-1057, the reasonable inference the magistrate judge would have drawn was that this single second corresponded to a visit to the website's homepage and nothing more.

Second, Special Agent Ford knew that one of the residents of the Sanders home was a licensed clinical psychologist who worked with both adults and children and that the IP address in question was assigned to that clinical psychologist. Special Agent Ford had recorded this information in the FD-1057 but failed to include it in the warrant. Had he included it, a reasonable inference would have been that a single visit to the website, at a single time, was done in the course of the licensed clinical psychologist's work. This fact, especially when considered

[6] The FBI has previously used such Network Investigative Techniques, or malware, in other cases. *See, e.g., United States v. Darby*, 190 F. Supp. 3d 520 (E.D. Va. 2016), *aff'd*, 721 F. App'x 304 (4th Cir. 2018); *United States v. Matish*, 193 F. Supp. 3d 585 (E.D. Va. 2016); *United States v. McLamb*, 220 F. Supp. 3d 663 (E.D. Va. 2016), *aff'd*, 880 F.3d 685 (4th Cir. 2018).

in combination with the absence of an allegation that any of the residents had a criminal history, was material.

Finally, Special Agent Ford misled the magistrate judge by failing to provide context for the term "twink," which would have helped the magistrate understand that the target website was not all child pornography but instead contained a mix of legal and illegal content. A "twink" is "[a] slang term used to describe a young or young-looking *man* with little or no facial or body hair." *Terminology*, Montclair State University LGBTQ Center, https://www.montclair.edu/lgbtq-center/lgbtq-resources/terminology/ (last visited May 28, 2020) (emphasis added); *see also Twink (gay slang)*, Wikipedia, https://en.wikipedia.org/wiki/Twink_(gay_slang) (last accessed May 28, 2020) ("Twink is gay slang for *a young man in his late teens to early twenties* whose traits may include: general physical attractiveness; little to no body or facial hair; a slim to average build; and *a youthful appearance that may belie an older chronological age*") (emphasis added).

4. Special Agent Ford misled the magistrate judge by mischaracterizing Tor and how it is used.

The affidavit is further misleading due to Special Agent Ford's mischaracterizations of Tor. Dr. Miller would proffer that the affidavit generally misled the magistrate judge in its characterization of Tor software and the Tor network. Special Agent Ford claimed that "because accessing the [target website] required numerous affirmative steps by a user—including downloading Tor software, accessing the Tor network, finding the web address for the [target website], and then connecting to the [target website]," the affiant asserted that it was "extremely unlikely that any user could simply stumble upon the [target website] without understanding its purpose and content." (Affidavit ¶¶ 27, 29).

First, contrary to what was suggested in the affidavit, using Tor is not suspicious. While Special Agent Ford characterized the Tor Project as "the private entity that maintains the Tor network," he knew or should have known that The Tor Project is a 501(c)(3) U.S. nonprofit organization whose mission is to "[t]o advance human rights and freedoms by creating and deploying free and open source anonymity and privacy technologies, supporting their unrestricted availability and use, and furthering their scientific and popular understanding." *Browse Privately. Explore Freely,* The Tor Project, https://www.torproject.org (last accessed June 7, 2020).

The Tor network is not exclusively or primarily intended for illegal activities, and because it is publicly accessible and because many people legitimately use the Tor network, the affiant knew or should have known that someone could stumble across the website without knowing what content it contained. While courts have recognized the anonymity protections of Tor, it is wrong to conclude that the use of these protections reflects a fair probability of criminal intent. As this Court has previously acknowledged, "[t]he U.S. Naval Research Laboratory created the Tor network in an attempt to protect government communications. The public now can access the Tor network. Many people and organizations use the Tor network for legal and legitimate purposes." *Matish*, 193 F. Supp. 3d at 593.

Fox News compared which was the best of different web browsers and gave the Tor browser an honorable mention: Fox News reported that the "Tor Browser is one of the best anonymous web browsers out there. It's so reliable, in fact, that people living under repressive

governments have used it to break through censorship. . . if you're looking for the safest, most private way to browse the net, Tor might be your go-to." *Which browser is best? Comparing Chrome, Safari, Firefox, Edge, and Tor*, Fox News, https://www.foxnews.com/tech/which-browser-is-best-comparing-chrome-safari-firefox-edge-and-tor (last accessed June 7, 2020). Furthermore, Fox News noted that while Apple Safari and Microsoft Edge are the "default" browsers that usually "come bundled with new computers, . . . they tend to lack some of the security features and extensions" found in other browsers one can download. *Id.* Fox News further counselled against using a default browser such as Internet Explorer, giving it a dishonorable mention, in part because it is "an absolute minefield for malware." *Id.*

In this case, the magistrate judge was not able to consider the many legal reasons why people would seek to anonymize their online activity by using a Tor network, as the affiant omitted such material information from the affidavit. For example:

> Many people don't want the things they say online to be connected with their offline identities. They may be concerned about political or economic retribution, harassment, or even threats to their lives. Whistleblowers report news that companies and governments would prefer to suppress; human rights workers struggle against repressive governments; parents try to create a safe way for children to explore; victims of domestic violence attempt to rebuild their lives where abusers cannot follow.

Anonymity, Electronic Frontier Foundation, https://www.eff.org/issues/anonymity (last accessed June 2, 2020).

Anonymizing online activities can enable people to more freely communicate, organize, and associate with others. Using a Tor browser can create space for people to develop and share ideas. In particular, people who are members of minority groups who may fear discrimination or harassment on the basis of their sexual orientation, ethnicity, race, religion, or gender identity can feel more empowered to exercise their First Amendment rights in such spaces.

Second, contrary to what was suggested in the affidavit, it does not require technical sophistication to download or use Tor, and the steps required to use and download Tor are the same regardless of whether someone is using Tor for legal or illegal reasons. It takes less than 15 seconds to download the Tor browser from The Tor Project's website, in only two clicks of the mouse. *See, e.g., Defend yourself: protect yourself against tracking, surveillance, and censorship*, The Tor Project, https://www.torproject.org/download/ (last accessed June 8, 2020). The steps required to download the Tor browser are as simple and straightforward as downloading any other browser that does not come automatically bundled with a new computer, like FireFox or Google Chrome. Once the Tor Browser was downloaded and opened, it appeared like any other web browser, and there was a search bar where one could search for content. *See, e.g.,* Screenshot of the Tor Browser, attached as Exhibit A. Dr. Miller would testify to the ease with which one can download and use Tor. *See also* Am. Civ. Liberties Union, *Challenging Government Hacking in Criminal Cases* 3 (Mar. 2017), https://www.aclu.org/sites/default/files/field_document/malware_guide_3-30-17-v2.pdf ("[u]sing Tor to browse anonymously or connect to hidden services is relatively straightforward and does not require a high level of technical sophistication. In fact, following simple instructions, most Internet users can do it within five minutes"). Someone who wanted to use Tor for perfectly legitimate reasons would easily follow the exact same steps described in the affidavit.

Third, contrary to what was suggested in the affidavit, a Tor browser can be used to access sites on the open Internet, there are Tor-based search engines, and it is possible to perform searches for content of websites on a Tor browser. The Tor browser allows a person to search for terms and access websites, including those available on the open-Internet. For example, one can search for the Department of Justice and pull up results that are indexed by search engines like DuckDuckGo or Google. *See, e.g.*, Screenshot of Search Results for "Department of Justice," attached as Exhibit B. DuckDuckGo can also be used to search for hidden websites. A user can also employ a Torch Search engine, which can be found simply by searching it for on DuckDuckGo, to search hidden websites. *See, e.g.,* Screenshot of Torch Search Engine, attached as Exhibit C, and Screenshot of Search Results for "Department of Justice" on Torch Search Engine, attached as Exhibit D. Indeed, the "Tor browser is similar to a normal web browser in many ways. It's no more difficult to use than Google Chrome or Microsoft Edge. The difference is that Tor browser connects you to the internet through the Tor network." *The Ultimate Guide to Tor Browser (with Important Tips) 2020,* VPN Mentor, https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/ (last accessed June 7, 2020).

Fourth, contrary to what was suggested in the affidavit, while there are ways for a person to allow themselves to be de-anonymized on Tor, the intent of Tor is to protect people's anonymity. Special Agent Ford alleged that "in the Tor Project's FAQ [Frequently Asked Questions], the question 'So I'm totally anonymous if l use Tor?' is asked, to which the response is, in bold text, 'No.'" But this was not how the Tor Project's FAQ appeared in 2020; accordingly, we are doubtful that the website appeared that way in February 2020. *Cf. Most Frequently Asked Questions*, Tor Project, https://support.torproject.org/faq/ (last accessed June 8, 2020) ("Am I totally anonymous if I use Tor? Generally it is impossible to have perfect anonymity, even with Tor. Though there are some things you can practice to improve your anonymity while using Tor and offline"). When browsing on Tor, unless someone reveals their identity (which was not alleged here), their anonymity should be protected. *See, e.g., Id.* ("If you visit a website using Tor Browser, they don't know who you are or your true location. Unfortunately many sites ask for more personal information than they need through web forms. If you login to that website, they still don't know your location but they know who you are. Further, if you provide: name, email, address, phone number, or any other personal information, you are no longer anonymous to that website"). Thus, while a locked safe is meant to protect one's personal belongings, someone can undermine the intended protections that safe provides by sharing information that would reveal the combination to unlock the safe. However, there were no facts alleged here that would suggest the Internet user de-anonymized themselves and therefore undermined the protections available to them.

Special Agent Ford was, in effect, asking the magistrate judge to read suspicion into innocent and natural conduct that many people engage in, which is downloading and using a Tor browser. Had the affiant provided a more accurate characterization of Tor, the magistrate judge would have understood that the "affirmative steps" of "downloading Tor software" and "accessing the Tor network" do not support a finding of probable cause. (Affidavit ¶ 29). For example, someone could download and use the Tor Browser to access Facebook to browse anonymously, including to avoid the targeted ads and personal data tracking that occurs on less protective browsers. *See, e.g.,* Facebook https://www.facebookcorewwwi.onion/ (last accessed June 8, 2020); Screenshot of Tor Facebook Page attached as Exhibit E. The magistrate judge would also have understood that because Tor is widely used for a variety of legitimate purposes,

and because links to websites can be shared broadly, the mere accessing of a website address does not mean that a person found it the same way as law enforcement.

5. Special Agent Ford misled the Magistrate Judge about places where evidence of wrongdoing might reasonably be found.

Special Agent Ford relied on generalized statements such as, "[d]igital information can be automatically stored in many places," or that "a computer user's Internet activities generally leave traces or 'footprints' in the web cache and history files . . . until overwritten by other data," to suggest that evidence of wrongdoing could be found on any electronic device in the Sanders's home. (Affidavit ¶ 36(h)). However, such statements wrongly implied that activity on a Tor browser, with its heightened anonymity protections, would leave such traces after a single visit or that any traces of a single visit would remain on a device more than eight months later. Special Agent Ford knew or should have known this was not the case. According to the Tor Project's website, which Special Agent Ford had reviewed, the "Tor Browser is designed to prevent websites from 'fingerprinting' or identifying you based on your browser configuration. By default, Tor Browser does not keep any browsing history. Cookies are only valid for a single session (until Tor Browser is exited or a New Identity is requested)." *About Tor Browser,* The Tor Project, https://tb-manual.torproject.org/about/ (last accessed June 8, 2020).

Special Agent Ford knew or should have known that more than eight months later, it was unlikely that any electronic storage device would contain evidence of the Internet activity a user engaged in on May 23, 2019, using a Tor browser. If it had, the scope of the search should have been circumscribed to the particular folders of cached files within particular electronic storage devices where there was probable cause to believe that specific files, reflecting traces, if any, of the May 23, 2019, visit, could have been found. However, it is unlikely that the Tor browser would have saved any of that information in the first place.

Thus, especially when the material false or reckless statements are excised from the affidavit, and when the material omissions are included, no magistrate judge could find probable cause to justify the search. For these and other reasons, the good faith exception to the warrant requirement would not apply.

***

As noted, we would like to schedule a time to meet (virtually or via telephone) to discuss this matter further; please just let us know a convenient time for you. Thank you in advance for your courtesy.

Sincerely,

Jonathan Jeffress

KaiserDillon PLLC
1099 14th Street NW, 8th Floor - West
Washington, D.C. 20005
(202) 640-4430

EXHIBIT A: Screenshot of the Tor Browser

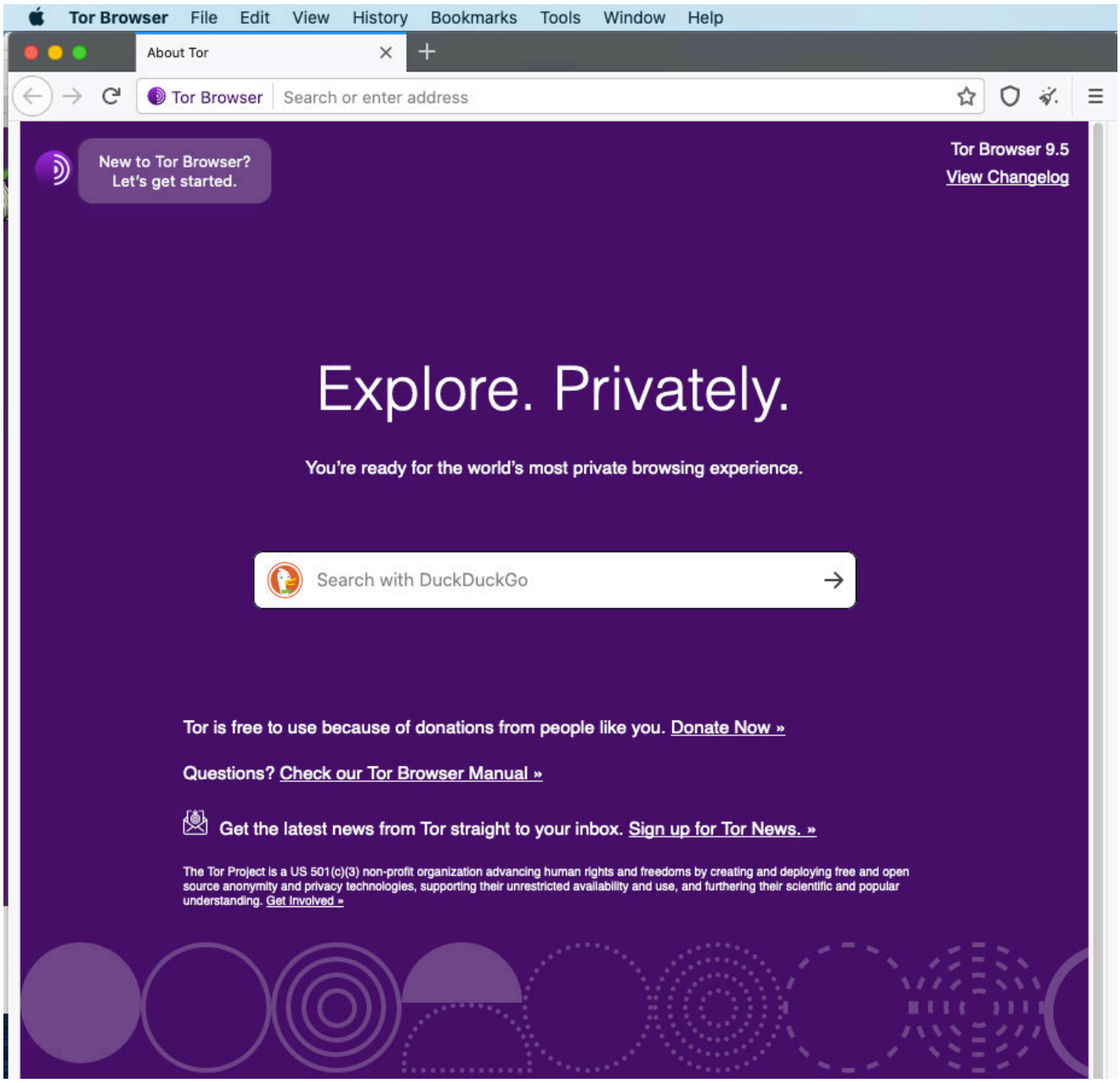

EXHIBIT B: Screenshot of Search Results for "Department of Justice"

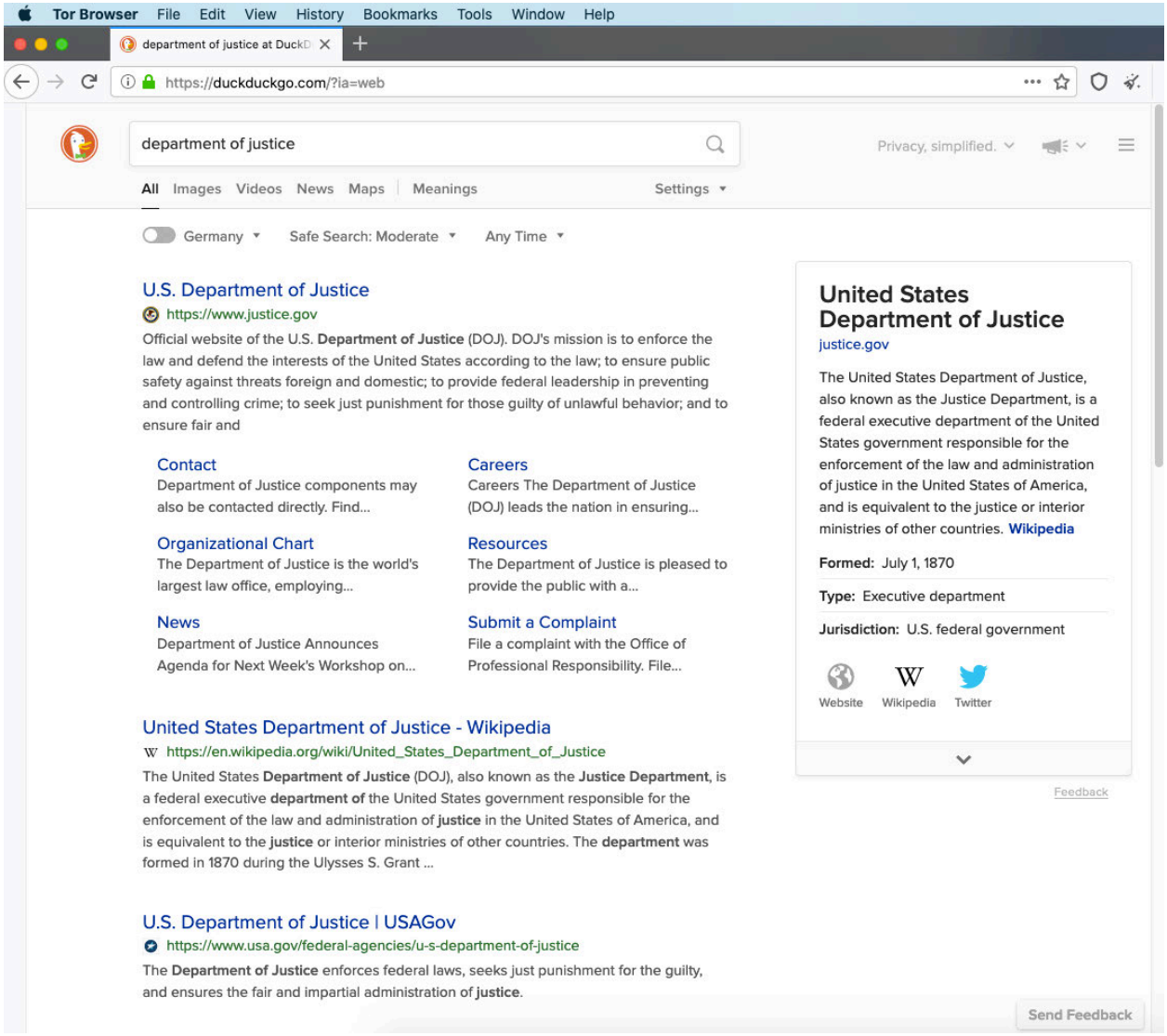

Exhibit C: Screenshot of Torch Search Engine

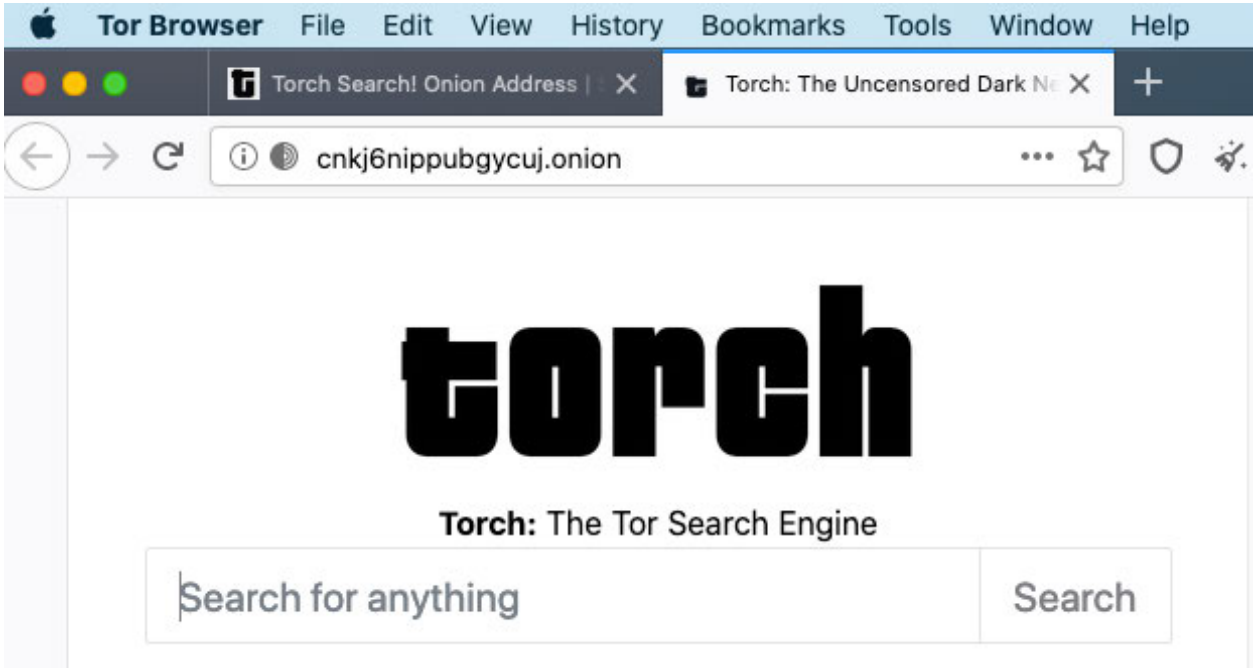

Exhibit D: Screenshot of Search Results for "Department of Justice" on Torch Search Engine

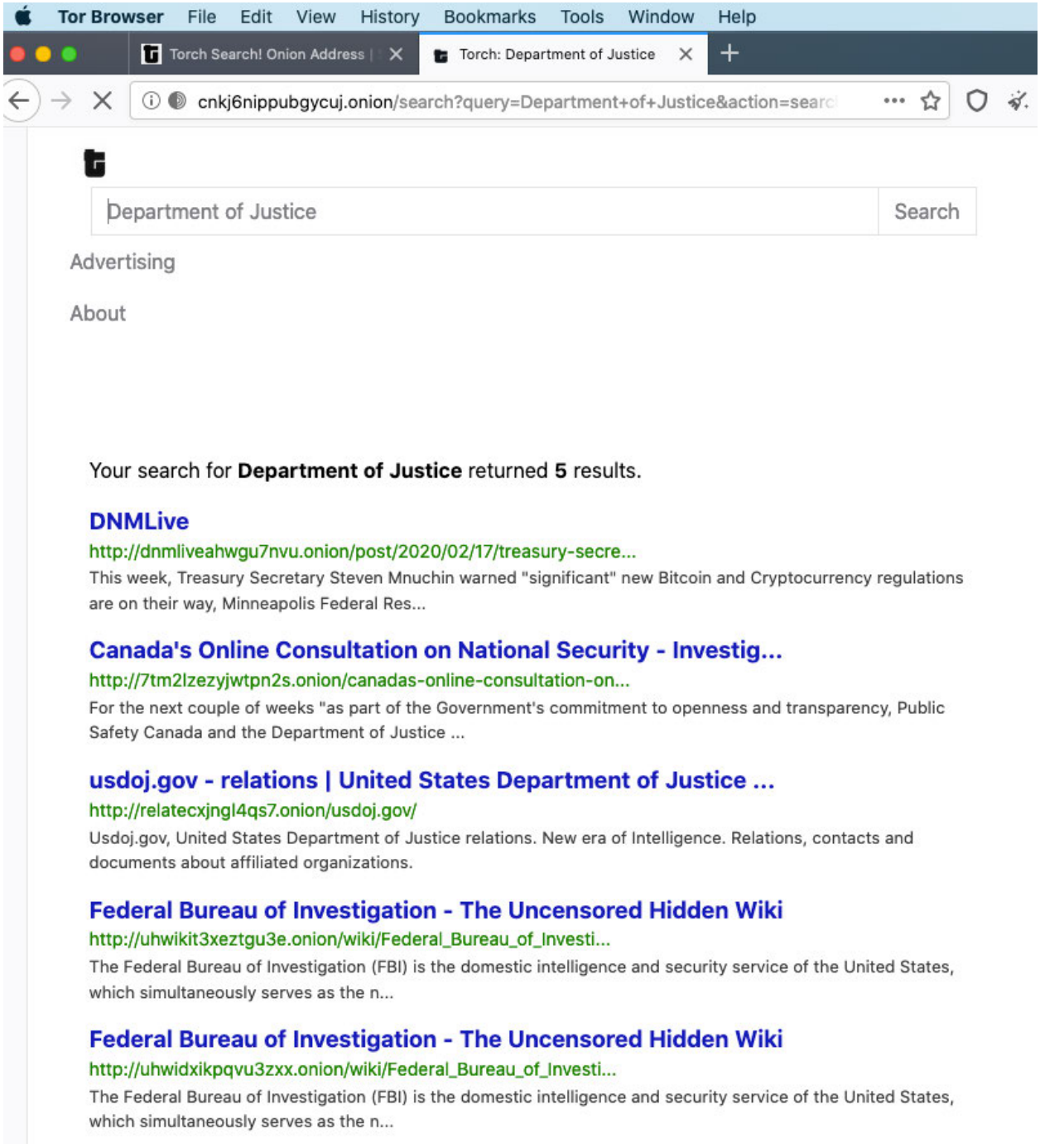

Exhibit E: Screenshot of Facebook Tor Website